Security Enhancement of Single Sign on Mechanism for Social Media Networks(SMN)

Miss. Bobade Snehal [1], Mr.Joshi Vishnu [2],
Mr. Godage Somnath [3],Miss. Patil Swati [4]

[1]Student,Computer Dept.,SPCOE, Pune, Maharashtra, India,
[2]Student,Computer Dept.,SPCOE, Pune, Maharashtra, India,
[3]Student,Computer Dept.,SPCOE, Pune,Maharashtra, India,
[4]Student,Computer Dept.,SPCOE, Pune,Maharashtra, India,

Email: vishmjoshi@gmail.com[1] ,godagesomnath2@gmail.com.com[2]

Abstract-It is usually not a piratical by asking one user to maintain number of pairs of identity and password for different service provider ,since this could increase the work load of both users and service providers as well as the communication overhead of networks . To tackle this problem , the single sign on mechanism (SSO) is introduce. Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a Social media Network(SMN). Recently, Proposed mechanism allows user to sign on only once and have their identities automatically verified by each application or service they want to access afterwards. Thegoalofasinglesignonplatformisto eliminate individual sign on procedures by centralizing user authentication and identity management at a central identity provider. In this SSO system, user should seamlessly authenticated to his multiple user accounts (across different systems) once user proves his/her identity to the identity provider..

Index Terms--Facebook ,twitter ,gmail ,SSO(single sign on),information security,security analysis,Social media networks.

1. INTRODUCTION

A single Sign-on infrastructure provides transparent access to all network resources for a user with only a single login. It enables a user to access multiple computer platforms or application systems after being authenticated just one time [1]. The user's identity and authorization data is stored in this centralized setup (of 1 or more servers), which is trusted by all applications.

Single sign on can be implemented either as a common authentication/authorisation service with centralised identity management. This provides a common centralised infrastructure to which both users and hosts communicate to authenticate accesses to resources

2. RELATED WORK:-

In 2000, Lee and Chang [2] proposed a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu [3] pointed out that Lee-Chang scheme is insecure against both impersonation attack and identity disclosure attack.Courtney Powell et al. [3]implemented a prototype of the proposed system and confirmed its efficacy. In the experiment conducted,verified that SSO was operational between two locations, Kitami Institute of Technology and Hokkaido University. In addition, by using this authentication infrastructure and the adopted GSI technique,plan to construct an SSO system. Quantitative measurements such as authentication delay and security threats are among other related aspects that will also be considered. Faraz Fatemi Moghaddam et al. [4] The proposed model was designed and described by establishing two cloud servers for storing encrypted account details and cryptography keys. Moreover, a cloud-based SaaS application was designed to connect clients and SaaS service providers. Using AES256 and SSL in the suggested model improves the security of cloud-based SSO algorithm. In conclusion, the reliability of the proposed model has been assured for storing users important data according to specificationsof the model.Yang Jian et al.[5] The increased two data flows that are from AS (authentication server) to TGS (ticket-granting Server) and from TGS to app servers V (Ticket), which are used to transmit the ticket-granting ticket and the service-granting ticket, they are greatly reduced the clients security risks and its workload, and enhanced the clients work efficiency through regulating the topological structure of the system and adjustment of the information flows. The new added authentication client database can dynamically register authenticated client information, and new added authorization client database can dynamically register authorized client information .Jian Hu et al. [6] Through the single sign-on project construction, a unified database of persons was established. integrated the isolated system that is not only convenient for the customer but also convenient the manager. In the construction of the Digital Campus Enterprise Service Bus was also used to achieve synchronization of information between databases.Jianhong Zhang et al.[8] Single-sign-on is a new technique thereby increases the usability of the network as a whole and at the same time centralizes the management of relevant system parameters. Unfortunately,show that Ren's scheme is suffering unforgivable attack we proposed in this paper. Namely, any one without a legal ID can pass the verification. Finally,give the corresponding revise. Ren's scheme was very efficient Single-sign-on formula for authentication in computer networks. Thus, it is an open problem to improve Ren's scheme and make it secure in the standard model. David J. Boyd et al. [9] The proposed method could improve the protection for the card, the cardholder and the service provider(s). No form of authentication is perfect because that authentication is only true at that point in time and its strength is also dependentonotheexternalfactors. Whethertheauthenticationissufficient for the business need; the userˆas privacy is enhanced, the user control any release of personal information. Spoorthi V.et al.[10]The Solution explainedcanprovidestrongclientsideauthenticationinSingleSign-On domains. It has been proposed to be a Native app-friendly standard as it does not require a browser to authenticate. Also, multiple numbers of native apps can actually be managed using a single Mobile SSO Agent at the mobile device. It is a user friendly authentication mechanism as it does not involve multifactor authentication or one time password, which decreases user acceptance of cloud. The access can be revoked to a particularuserat anytimejustbyrevokingthenorrespondingcertificate. The proposedsystemcanalsimprovebandwidthefficiencyofthecommunication protocol, as only the certificate address is sent over network.

3. PROBLEM STATEMENT:

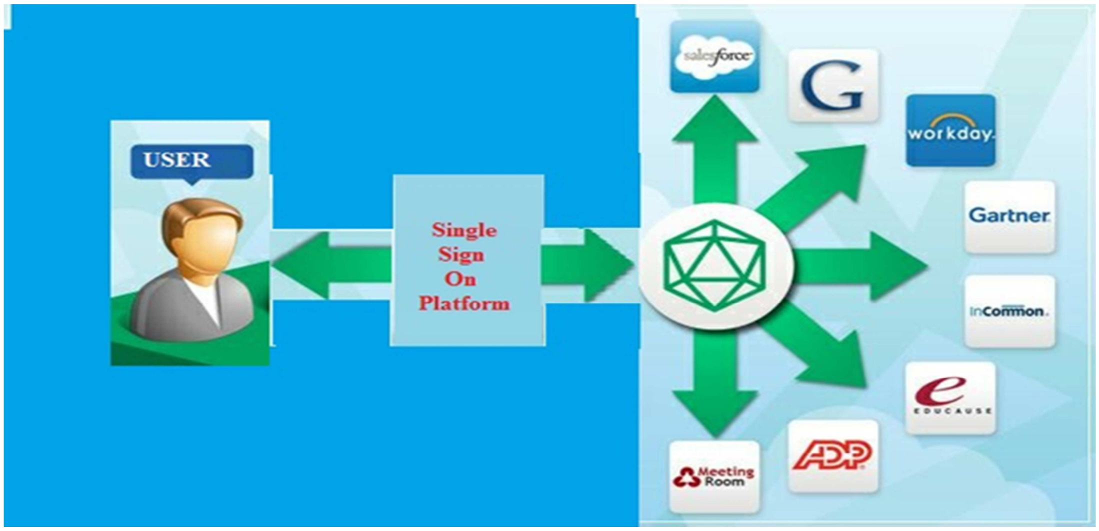
It is usually not a piratical by asking one user to maintain number of pairs of identity and password for different service provider ,since this could increase the work load of both users and service providers as well as the communication overhead of networks . To tackle this problem , the single sign on mechanism (SSO) is introduce.

4.PROPOSED SYSTEM:-

1. The Friend Relationship-Based User Identification This will help for finding relation between different sites or different social site users.

2. Single sign in on user identifications of different domain Authenticate Once To Access Many. Login Credentials (ID And Authentication) Usually Stored Locally. Transparently Presented to the System or Application When Needed.

3. Cross platform identifications To check pair on different site or SMN.



Single Sign On Architecture 1

5.ALGORITHM:-

Single Sign on use Following Algorithms.

1. DES,AES Algorithm.
2. Encryption & Decryption Algorithm.

Functions:-

A. System Initialization Phase:-

B. Registration Phase .:-

C. User Identification Phase :-

D. Encryption and Decryption Phase:-

Encryption and Decryption between user and provider is ensured using AES algorithm which is more secure than DES and there are currently no known nonbrute force attacks against AES. Data which is send from each provider to user is encrypted and send to the user, then the user decrypts it and the original data is retrieved. All these encryption and decryption are done using the more secure Advanced Encryption Algorithm (AES).

6. MATHEMATICAL MODEL:-

System Description:-
Input:-
User Name:
Password:

Output:-
AuthorizedData from WEB.

Success Condition:-
Single sign-on (SSO) is a mechanism whereby a single action of user authentication and authorization can permit a user to access other applications and systems where he/she has access, without the need to enter multiple user IDs and passwords.

Failure Conditions:-
- Internal Server Error
- Unexpected Error
- File Not Found Error
- Authentication Failed

7.METHODOLOGY

In the existing system, different security schemes are proposed by many researchers. In the proposed system, various Client-Server programs are written to implement the project using socket programming in Java. This work uses the multithreading features of Java to run in parallel for different providers. Chang-Lee algorithm is used for user identification phase. But, it is using a less secure DES algorithm. This paper user a more secure AES algorithm to enhance the security features. So, this scheme is more secure than Chang-Lee scheme

8. DEVELOPMENT ENVIRONMENT:-

The proposed system requires Eclipse that is an open source software development environment. Eclipse consists of an Extensible plugin system and an IDE. The Android project has been developed in the Helios version of Eclipse, as it has plugins that are mainly used for Android.

8. 1 Android SDK

Integrated Development Environment (IDE) is used in Android development in order to make it more straight forward and quick. It has been recommended for the developers because of its simplicity in working. Android is basically a multitasking platform. To give an example, the application has one application for navigation, another application for games, and another messaging. These applications can work simultaneously because of this multitasking ability of the Android platform.

8.2 ADT Plugin

ADT (Android Development Tools) is a plugin developed by Google. Its main purpose is for developing Android mobile applications in Eclipse. It makes it easy and convenient for all the Android developers working in Eclipse environment to quickly create Android projects and debug the programs whenever needed.

Text editor should not be used in the development of large applications having a large amount of code as the text editor cannot highlight wrong spellings.

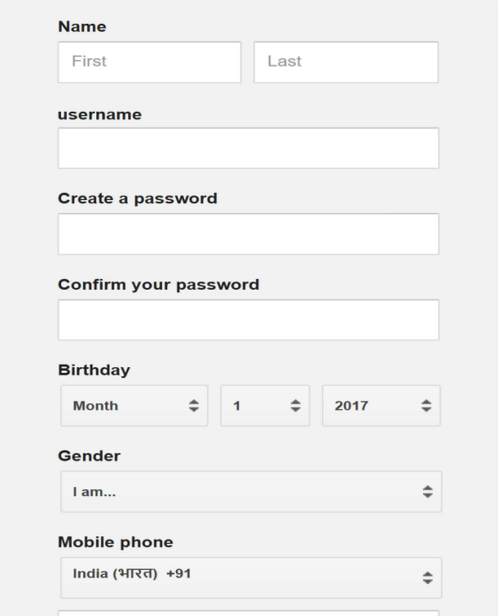
8.3 Android Emulator

Android emulator is a virtual mobile device which is included in every Android SDK which runs on the users computer. Android emulators are used to test Android applications, so there is no need of any physical device.

Android emulator supports Android Virtual Device (AVD) configuration, which in itself is an emulator containing specific Smartphone Operating System. Using AVD, one can easily test his applications.

Any application running on an emulator can use the services provided by the Android platform like play audio, store or retrieve data etc. But with these features comes a few limitations. Neither does it support Bluetooth, nor does it support SMS/MMS communication.

10. RESULT:



Name
First | Last

username

Create a password

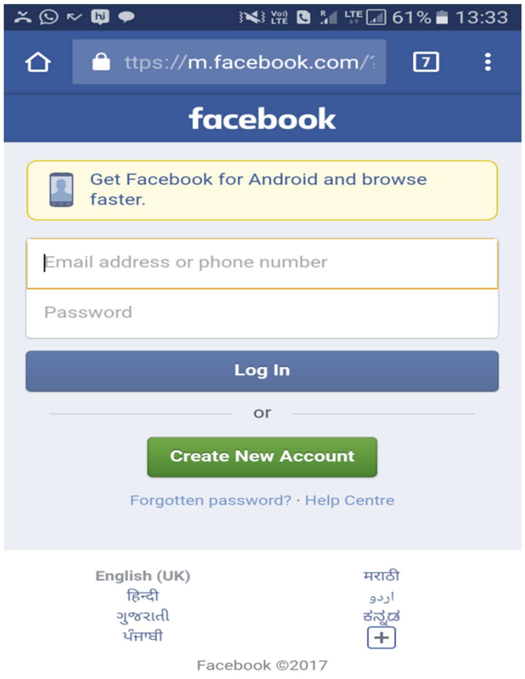
Confirm your password

Birthday
Month | 1 | 2017

Gender
I am...

Mobile phone
India (भारत) +91

Registration Page 1



61% 13:33

ttps://m.facebook.com/

facebook

Get Facebook for Android and browse faster.

Email address or phone number

Password

Log In

or

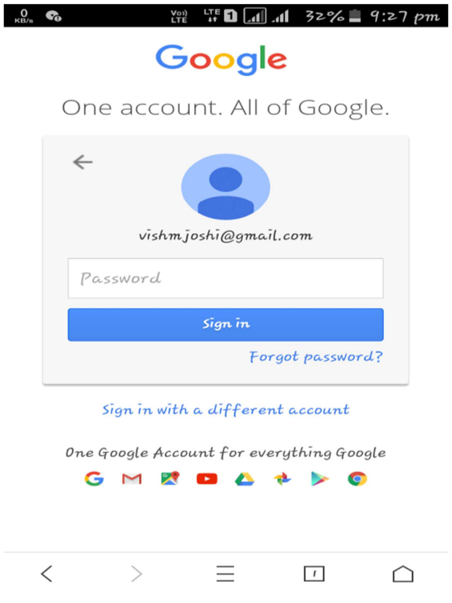
Create New Account

Forgotten password? · Help Centre

English (UK) मराठी
हिन्दी اردو
ગુજરાતી ಕನ್ನಡ
ਪੰਜਾਬੀ

Facebook ©2017

FaceBook Login Page 1



32% 9:27 pm

Google

One account. All of Google.

vishmjoshi@gmail.com

Password

Sign in

Forgot password?

Sign in with a different account

One Google Account for everything Google

Gmail Login Page 1

8. CONCLUSIONS:-

The problem of user identification across SMN platforms and o□ered an innovative solution.Single Sign-On enables users to login quickly and securely to all their applications, websites and mainframe sessions with just one identity

11. ACKNOWLEDGEMENT:-

I would like to take this opportunity to express my sincere gratitude to my project guide & head of department Prof. Deokate G.S his encouragement,guidance,and insight throughout the research and in the preparation of this dissertation,he truly exemplifies the merit of technical excellence and academic wisdom.his extensive knowledge,serious research attitude and encouragement were extremely valuable to me.I also appreciate not only for his professional,timely and valuable advices,but also for his continuous scheduled follow up and valuable comments during my research work.I should also like to acknowledge the contribution of my principal Dr.G.U.Kharat.

Appendix A.

Appendices should be used only when absolutely necessary. They should come after the References. If there is more than one appendix, number them alphabetically.

REFERENCES

[1] Wikipedia,”SSO,”http://en.wikipedia.org/wiki/SSO. 2014.

[2] Ashish G. Revar, Madhuri D. Bhavsar, Securing User Authentication using Single SignOn in Cloud Computing, INSTITUTE OF TECHNOLOGY, UNIVERSITY, AHMEDABAD 382 481, 08-10 DECEMBER, 2011.

[3] Courtney Powell, Takashi Aizawa, Masaharu Munetomo, Design of an SSO Authentication Infrastructure for Heterogeneous Inter-cloud Environments, 2014 IEEE 3rd International Conference on Cloud Net

[4] Faraz Fatemi Moghaddam, Omidreza Karimi and Mostafa Hajivali, Applying a Single Sign-On Algorithm Based on Cloud Computing Concepts for SaaS Applications, 2013 IEEE 11th Malaysia International Conference on Communications, 26th - 28th November 2013, Kuala Lumpur, Malaysia.

[5] Yang Jian, An Improved Scheme of Single Sign-on Protocol, 2009 Fifth International Conference on Information Assurance and Security.

[6] Jian Hu, Qizhi Sun, Hongping Chen, APPLICATION OF SINGLE SIGN-ON (SSO) IN DIGITAL CAMPUS. 9781-4244-6769-3/10/26.00 2010 IEEE

[7] Sahana K. Bhosale,"Architecture of a Single Sign on (SSO) for Internet Banking", IET International Conference on Wireless, Mobile and Multimedia Networks, 2008.

[8] Jianhong Zhang and Xue Liu,"On the Security of An Identity-based Single-sign-onScheme",978-1-4244-55409/10/26.00 ˆ A c
2010IEEE.

[9] DavidJ.Boyd,"SingleSign-OntotheWebwithanEMVCard",9781-4244-2249-4/08/25.00 ˆ A c
2008 IEEE. XX

[10] Spoorthi V and K. Chandra Sekaran,"Mobile Single Sign-On SolutionforEnterpriseCloudApplications",9781-4799-3486-7/14/31.00 c2014 IEEE